

ZTW  
AP

THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants : 09/656,815  
 Applicants : Rodriguez et al.  
 Filed : September 7, 2000  
 Art Unit : 3624  
 Examiner : Colbert, Ella  
 Docket No. : B-68149(014354/0004)  
 Customer No. : 33649

Confirmation No. 1848

Mail Stop Appeal Brief - Patents  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, VA 22313-1450

Certificate of Mailing Under 37 C.F.R. 1.8(a)

I hereby certify that these documents are being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on September 14, 2006.

*Joan B. Faragher*  
 Joan B. Faragher

**ATTENTION: Board of Patent Appeals and Interferences**

**TRANSMITTAL OF APPEAL BRIEF**

In response to the Notification of Non-Compliance with the Requirements of 37 CFR 41.37, enclosed is the substitute Appellant's Brief. A check in the amount of \$500.00 was filed with the original Appellant's Brief on August 8, 2006. This Appellant's Brief is timely filed within the 30-day period set forth with the mailing of the Notification on August 30, 2006. Therefore, no fees are believed due with the filing of this substitute Appellant's Brief; however, the Commissioner is hereby authorized to charge any additional fee or credit any refund to the deposit account of Jackson Walker L.L.P., No. 50-1752.

Dated: September 11, 2006

Respectfully submitted,

JACKSON WALKER L.L.P.

By: 

Christopher J. Rourk  
Reg. No. 39,348

901 Main Street, Suite 6000  
Dallas, Texas 75202  
Telephone: (214) 953-5990  
Facsimile: (214) 661-6604  
E-Mail: [crourk@jw.com](mailto:crourk@jw.com)



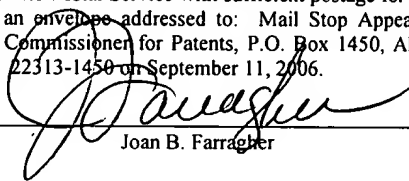
**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BOARD OF PATENT APPEALS AND INTERFERENCES**

Appl. No. : 09/656,815 Confirmation No. 1848  
 Applicants : Rodriguez et al.  
 Filed : September 7, 2000  
 Art Unit : 3624  
 Examiner : Colbert, Ella  
 Docket No. : B-68149(014354/0004)  
 Customer No. : 33649

Mail Stop Appeal Brief - Patents  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, VA 22313-1450

Certificate of Mailing Under 37 C.F.R. 1.8(a)

I hereby certify that these documents are being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on September 11, 2006.

  
 Joan B. Farragher

**ATTENTION: Board of Patent Appeals and Interferences**

**APPELLANT'S BRIEF (37 C.F.R. 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on June 8, 2006 and the Final Office Action mailed March 2, 2006.

The fees required under § 1.17(c), and any required petition for extension of time for filing this brief and related fees are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

## TABLE OF CONTENTS

I	REAL PARTIES IN INTEREST (37 C.F.R. §41.37(c)(1)) .....	4
II	RELATED APPEALS AND INTERFERENCES (37 C.F.R. §41.37(c)(2)) .....	5
III	STATUS OF CLAIMS (37 C.F.R. §41.37(c)(3)).....	6
IV	STATUS OF AMENDMENTS (37 C.F.R. 41.37(c)(4)).....	7
V	SUMMARY OF THE CLAIMED SUBJECT MATTER (37 C.F.R. 41.37(c)(5)) .....	8
VI	GROUNDS OF REJECTION TO BE REVIEWED UPON APPEAL (37 C.F.R. §41.37(c)(6)).....	12
VII	ARGUMENTS (37 C.F.R. 41.37(c)(7)) .....	14
1.	The Examiner has improperly rejected claim 9 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention, as the Examiner has established that the claim term is not insolubly ambiguous. ....	14
2.	The term “determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and transmitting the authorization request to the appropriate authorization system” is not insolubly ambiguous. ....	14
3.	The term “performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device” is not insolubly ambiguous. ....	15
4.	The terms “two or more authorization systems,” “two or more point-of-sale systems,” and “one or more point of sale systems” have proper antecedent basis. ....	15
5.	The Examiner has not properly rejected claims 9, 10, 13, 14, 17, 19, 22, 24 and 26-28 under 35 U.S.C. § 112, second paragraph, because the rejection refers to the specification. ....	16
6.	The Examiner has not identified the corresponding structure of the means plus function elements in claim 9, and there is no such structure or an equivalent in any of the cited art. ....	17
7.	The Examiner has not identified the corresponding structure of the means plus function elements in claim 10, and there is no such structure or an equivalent in any of the cited art. ....	21
8.	The Examiner has not identified the corresponding structure of the means plus function elements in claim 11, and there is no such structure or an equivalent in any of the cited art. ....	21
9.	The Examiner has not identified the corresponding structure of the means plus function elements in claims 12, 25 and 26, and there is no such structure or an equivalent in any of the cited art. ....	22
10.	The Examiner has not made a prima facie showing of obviousness in rejecting claims 9-11 and 17 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,500,890 to Rogge et al. (hereinafter “Rogge”) in view of U.S. Patent No. 5,448,047 to Nair et al. (hereinafter “Nair”).....	23

11.	The Examiner has not made a prima facie showing of obviousness in rejecting claims 12-28 under 35 U.S.C. § 103(a) as being unpatentable over Rogge and Nair in view of U.S. Patent No. 6,178,409 to Weber et al. (hereinafter “Weber”).	24
VIII	APPENDIX OF CLAIMS (37 C.F.R. 41.37(c)(8))	28
IX	EVIDENCE APPENDIX (37 C.F.R. 41.37(c)(9))	32
X	RELATED PROCEEDINGS APPENDIX (37 C.F.R. 41.37(c)(10))	33

The final page of this brief bears the practitioner’s signature.

**I REAL PARTIES IN INTEREST (37 C.F.R. §41.37(c)(1))**

The real party in interest in this appeal is:



the following party:

Paymentech L.P. by an assignment from BOPS Holdings, L.L.C. and PTI General Pa, Reel 013527, Frame 0849;

BOPS Holdings, LLC and PTI General Partner, L.L.C. by an assignment from Banc One Payment Services, L.L.C., Reel 013228, Frame 0124; and

Banc One Payment Services, L.L.C. by an assignment from Rodriguez et al., Frame 011090, Frame 0948.

## II RELATED APPEALS AND INTERFERENCES

### (37 C.F.R. §41.37(c)(2))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal:

4      ☒ there are no such appeals or interferences.

**III STATUS OF CLAIMS (37 C.F.R. §41.37(c)(3))**

**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 28

**B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims cancelled: Claims 1-8
2. Claims rejected: Claims 9-28.

**C. CLAIMS ON APPEAL**

The claims on appeal are: Claims 9-28.



**IV STATUS OF AMENDMENTS (37 C.F.R. 41.37(c)(4))**

No amendments have been submitted subsequent to the final rejection of the claims.

## V SUMMARY OF THE CLAIMED SUBJECT MATTER

### (37 C.F.R. 41.37(c)(5))

Claim 9 includes an apparatus for transmitting credit transaction data over a communications medium that comprises protocol translator means (Fig. 5, 506; Fig. 7; Fig. 8; page 17, line 9-17; page 21, line 20 to page 25, line 9) for receiving the credit transaction data from two or more point of sale systems according to two or more different transmission protocols, each transmission protocol associated with a different credit authorization system, and forming a credit transaction data message, and encryption means (Fig. 5, 502; Fig. 7; Fig. 8, page 16, line 11-25; page 21, line 20 to page 25, line 9) for receiving the credit transaction data message from a protocol translator and encrypting the credit transaction data message.

Claim 10 includes the apparatus of claim 9 further comprising device router means (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9) for transmitting authorization data received in response to the credit transaction data message to the one or more point of sale systems.

Claim 11 includes the apparatus of claim 9 further comprising management system interface means (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9) for storing a protocol module to the protocol translator.

Claim 12 includes the apparatus of claim 9 further comprising management system interface means (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9) for storing an encryption module to an encryption system.

Claim 13 includes a method for transmitting credit transaction data over a communications medium comprising receiving credit transaction data from two or more point of sale devices, each reading credit card data from a magnetic stripe of a credit card. A point-of-sale device data transmission protocol is determined for use in assembling the credit transaction data into an authorization request. The authorization request is then encrypted, and the encrypted authorization request is transmitted over the communications medium. The encrypted authorization request is then decrypted, and it is determined which of two or more authorization systems is the appropriate authorization system to provide the authorization request to. The authorization request is then transmitted to the appropriate authorization system. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 14 includes the method of claim 13 wherein receiving the credit transaction data from the point of sale device comprises receiving the credit transaction data in accordance with one or more of an ISO 8583 protocol or a Visa-K protocol. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 15 includes the method of claim 13 wherein encrypting the authorization request comprises encrypting the credit transaction data using an encryption module received from a hub manager. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 16 includes the method of claim 13 wherein transmitting the encrypted authorization request over the communications medium comprises transmitting the encrypted data in an HTTP format. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 17 includes a method for controlling the transmission of credit transaction data comprising transmitting one or more control messages to a remote hub, each control message adapted for one of two or more different point of sale devices. The control message is processed at the remote hub. A control function is performed on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 18 includes the method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises transmitting status data for the remote hub. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 19 includes the method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises transmitting status data for one or more point of sale devices connected to the remote hub. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 20 includes the method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises updating the remote hub with a protocol module to accommodate a new point of sale device. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 21 includes the method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises updating the remote hub with an encryption module. (Fig. 7; Fig. 8; page 21, line 20 to page 25, line 9)

Claim 22 includes a system for transmitting credit transaction data comprising two or more point-of-sale systems, each point-of-sale system using a proprietary data format to read credit card data from a magnetic stripe of a credit card and generate credit transaction data. A remote hub system coupled to a communications medium receives the credit transaction data from one or more of the point of sale systems, translates the credit transaction data from the proprietary data format to a predetermined data format, encrypts the translated credit transaction data, and transmits the translated encrypted credit transaction data over the communications medium. A gateway system coupled to the communications medium receives the encrypted translated credit transaction data, decrypts the encrypted translated credit transaction data, and transmits the translated credit transaction data to an authorization system. (Fig. 1; Fig. 2; Fig. 3; Fig. 7; Fig. 8; page 7, line 8 to page 14, line 27; page 21, line 20 to page 25, line 9)

Claim 23 includes the system of claim 22 further comprising a first authorization system coupled to the gateway system and a second authorization system coupled to the gateway system. The gateway system transmits the credit transaction data to the first or second authorization system based upon the translated credit transaction data. (Fig. 1; Fig. 2; Fig. 3; Fig. 7; Fig. 8; page 7, line 8 to page 14, line 27; page 21, line 20 to page 25, line 9)

Claim 24 includes the system of claim 22 wherein the remote hub system further comprises a protocol translator receiving the credit transaction data from each of the one or more point of sale systems according to the proprietary data format associated with each point of sale system. (Fig. 1; Fig. 2; Fig. 3; Fig. 7; Fig. 8; page 7, line 8 to page 14, line 27; page 21, line 20 to page 25, line 9)

Claim 25 includes the system of claim 22 wherein the remote hub system further comprises update means for receiving an encryption update and installing the encryption update on the remote hub system. (Fig. 1; Fig. 2; Fig. 3; Fig. 7; Fig. 8; page 7, line 8 to page 14, line 27; page 21, line 20 to page 25, line 9)

Claim 26 includes the system of claim 22 wherein the remote hub system further comprises update means for receiving an encryption update and installing the encryption update on one or more of the point-of-sale systems. (Fig. 1; Fig. 2; Fig. 3; Fig. 7; Fig. 8; page 7, line 8 to page 14, line 27; page 21, line 20 to page 25, line 9)

Claim 27 includes the system of claim 22 wherein the point-of-sale systems include one or more pre-existing point of sale systems that are configured to communicate using a public

switched telephone network telephone line. (Fig. 1; Fig. 2; Fig. 3; Fig. 7; Fig. 8; page 7, line 8 to page 14, line 27; page 21, line 20 to page 25, line 9)

**VI GROUNDS OF REJECTION TO BE REVIEWED UPON APPEAL****(37 C.F.R. §41.37(c)(6))**

1. Whether the Examiner has improperly rejected claim 9 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention, when the Examiner's own statements establish that the claim term is not insolubly ambiguous.

2. Whether the term "determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and transmitting the authorization request to the appropriate authorization system" is insolubly ambiguous.

3. Whether the term "performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device" is insolubly ambiguous.

4. Whether the terms "two or more authorization systems," "two or more point-of-sale systems," and "one or more point of sale systems" have proper antecedent basis.

5. The Examiner has not properly rejected claims 9, 10, 13, 14, 17, 19, 22, 24 and 26-28 under 35 U.S.C. § 112, second paragraph, because the rejection refers to the specification.

6. Whether the Examiner has identified the corresponding structure of the means plus function elements in claim 9, and whether there is any such structure or an equivalent in any of the cited art.

7. Whether the Examiner has identified the corresponding structure of the means plus function elements in claim 10, and whether there is any such structure or an equivalent in any of the cited art.

8. Whether the Examiner has identified the corresponding structure of the means plus function elements in claim 11, and whether there is any such structure or an equivalent in any of the cited art.

9. Whether the Examiner has identified the corresponding structure of the means plus function elements in claims 12, 25 and 26, and whether there is any such structure or an equivalent in any of the cited art.

10. Whether the Examiner has made a prima facie showing of obviousness in rejecting claims 9-11 and 17 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,500,890 to Rogge et al. (hereinafter “*Rogge*”) in view of U.S. Patent No. 5,448,047 to Nair et al. (hereinafter “*Nair*”).

11. Whether the Examiner has made a prima facie showing of obviousness in rejecting claims 12-28 under 35 U.S.C. § 103(a) as being unpatentable over *Rogge* and *Nair* in view of U.S. Patent No. 6,178,409 to Weber et al. (hereinafter “*Weber*”).

## VII ARGUMENTS (37 C.F.R. 41.37(c)(7))

**1. The Examiner has improperly rejected claim 9 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention, as the Examiner has established that the claim term is not insolubly ambiguous.**

A claim should not be held invalid under 35 U.S.C. 112, second paragraph if the “meaning of the claim is discernible, even though the task may be formidable and the conclusion may be one over which reasonable persons will disagree.” *Bancorp Servs., L.L.C. v. Hartford Life Ins. Co.*, 359 F. 3d. 1367, 1371 (Fed. Cir. 2004). When a claim “is not insolubly ambiguous, it is not invalid for indefiniteness.” *Marley Mouldings, Ltd. v. Mikron Industries*, 417 F. 3d. 1356, 1361 (Fed. Cir. 2005).

In rejecting claim 9 under 35 U.S.C. 112, the Examiner questions at page 3 of the Office Action mailed March 2, 2006 “[w]hat is forming the credit transaction data message? Is it the protocol translator or the transmission protocol forming the credit transaction message?” (Emphasis added). As the Examiner himself was able to determine that the meaning of the claim term is that a credit transaction data message is formed, the claim is not insolubly ambiguous. The Examiner’s only question is whether a protocol translator or transmission protocol performs that function, a question that is irrelevant, as limiting the method to the disclosed apparatus would be improper (in fact, the transmission protocol is applied by the protocol translator, see, e.g., specification at page 17, lines 9-17). The claim term is not insolubly ambiguous, and the rejection must be reversed.

**2. The term “determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and transmitting the authorization request to the appropriate authorization system” is not insolubly ambiguous.**

As discussed, under the proper standard for rejecting a claim under 35 U.S.C. 112, second paragraph, the Examiner bears a high burden of establishing that the claim must be insolubly ambiguous. The Examiner has failed to demonstrate why the claim term “determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and transmitting the authorization request to the appropriate



authorization system” is insolubly ambiguous. The Examiner only states “[o]nce the encrypted authorization request has been decrypted what happens to the decrypted authorization request? It is very vague from the claim language what happens next.” In fact, it is not vague – first, it is determined which of two or more authorization systems is the appropriate authorization system to provide the authorization request to, and next, the authorization request is transmitted to the appropriate authorization system. This is clearly the decrypted authorization request, as processing of an encrypted authorization request would not be possible. There is nothing in the claim language to suggest that the two steps that follow the decrypting step do not occur next, and the Examiner has provided no substantive basis for any other construction, much less a substantive reason why the claim is insolubly ambiguous. This rejection must also be reversed.

**3. The term “performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device” is not insolubly ambiguous.**

Yet again, the Examiner has failed to demonstrate why the claim term “performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device” is insolubly ambiguous. The Examiner only states “[w]hat happens to the control message once it has been processed? It is vague in the claim language what happens to the control message next.” Again, nothing in the subject language is vague – a control function is performed on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device. What happens to the control message is thus evidently clear from the plain wording of the claim, and the Examiner has provided no substantive reason why the claim is insolubly ambiguous. This rejection must also be reversed.

**4. The terms “two or more authorization systems,” “two or more point-of-sale systems,” and “one or more point of sale systems” have proper antecedent basis.**

The Examiner improperly rejects claims 13 and 22 based on antecedent basis, when in fact it appears that the Examiner has misunderstood the meaning of the term “antecedent basis.”

In rejecting claim 13, the Examiner states that “Claim 13 recites the limitation ‘two or more authorization systems’ in line 10 and it is not in any of the other limitations of this claim.” However, that is not a proper antecedent basis rejection. As discussed in M.P.E.P. 2173.05(e) and as no doubt well understood by the Board, a valid antecedent basis problem occurs when it is unclear as to what *prior* elements a claim term make reference, hence the term “antecedent.” Simply because the claim term is not used elsewhere in the claim does not create a problem with antecedent basis, and in the context of the claim, “determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and transmitting the authorization request to the appropriate authorization system” distinguishes the claim over the prior art, where no such determination is necessary because each authorization system uses its own transmission protocol. Whatever the Examiner’s concern is with this claim, it appears to relate to the rejection of the claim over the prior art and not to an antecedent basis problem.

In regards to “two or more point-of-sale systems,” and “one or more point of sale systems,” the actual terms are “two or more point-of-sale systems,” and “one or more of the point of sale systems.” Perhaps, as improperly stated by the Examiner, an antecedent basis problem might exist, but that is the exact reason why the claim term was amended in the response filed August 5, 2005, which the Examiner does not appear to have reviewed. These rejections must therefore also be reversed by the Board.

**5. The Examiner has not properly rejected claims 9, 10, 13, 14, 17, 19, 22, 24 and 26-28 under 35 U.S.C. § 112, second paragraph, because the rejection refers to the specification.**

The Examiner improperly turns to the Specification to reject claims 9, 10, 13, 14, 17, 19, 22, 24 and 26-28 under 35 U.S.C. 112, second paragraph. As the Board is no doubt well aware, the second paragraph of 35 U.S.C. 112 states “The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.” In contrast, it is the first paragraph of 35 U.S.C. 112 that states that the “specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use

the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.” As such, the Examiner’s reliance on the Specification as a basis for the rejection of claims 9, 10, 13, 14, 17, 19, 22, 24 and 26-28 appears to be a rejection under the first paragraph of 35 U.S.C. 112, and not the second paragraph. Perhaps, the Examiner means something different, but if the ground for rejection has not clearly stated, it is improper, as it is not up to the Applicants to come up with hypothetical grounds for rejection where the Examiner has failed to clearly state a valid ground for rejection. For example, perhaps the Examiner was looking at the use of “two or more point of sale systems” in claim 9 and “one or more point of sale systems” in claim 10, and believed that usage created a valid basis for rejection under 35 U.S.C. 112, second paragraph. However, there is no valid basis for the rejection of claim 10 under 35 U.S.C. 112, second paragraph in that case, as claim 9 states that “a credit transaction data message” is formed from credit transaction data from two or more point of sale systems – although the credit transaction data that is transmitted to the authorization system includes credit transaction data from two or more point of sale system, it would be clear to one of ordinary skill in the art that an authorization message sent in response could contain credit transaction data for one or more point of sale systems. As such, the claim is not insolubly ambiguous, and the disclosure from the Specification is irrelevant as to the hypothetical rejection under 35 U.S.C. 112, second paragraph. The Applicants could spend a great deal more time trying to hypothesize what the Examiner may have been objecting to, but there is simply no duty for the Applicants to do so if the Examiner has failed to clearly state a legitimate basis for rejecting the claims. It is further noted that the Examiner has understood the claims well enough to reject all of them over prior art. Reversal of this rejection by the Board is also required.

**6. The Examiner has not identified the corresponding structure of the means plus function elements in claim 9, and there is no such structure or an equivalent in any of the cited art.**

The construction of the claims adopted by the Examiner is incorrect, and is used to improperly reject the claims. Claim construction is a question of law, and is reviewed *de novo*. *Markman v. Westview*, 52 F. 3d 967, 34 USPQ2d 1321 (Fed. Cir. 1995), *aff’d* 116 S.Ct. 1384 (1996).

No analysis of the claimed means plus function elements has been provided by the Examiner. Under controlling Federal Circuit precedent, when a means plus function clause invokes 35 U.S.C. 112, paragraph 6, the corresponding structure must be identified in the specification of the pending application, and that structure or an equivalent thereof must be identified in the prior art. *See, e.g., WMS Gaming, Inc. v. Int'l Game Technology, 184 F.3d 1339, 1349 (Fed. Cir. 1999)*, which holds that:

In a means-plus-function claim in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, ***the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm.*** The “special purpose computer” results from the computer being “programmed to perform particular functions pursuant to instructions from program software.”

(emphasis added) *See also* M.P.E.P. 2182-83. The Examiner has utterly failed to not only identify the disclosed structure in the pending application, but also to identify whether that disclosed structure or any equivalent thereof is present in the cited prior art. While this may be attributed to an oversight by the Examiner, it is in fact apparent that the Examiner would have failed to perform this analysis in any event because the corresponding structure disclosed in the specification or any equivalent thereof are entirely missing from the cited prior art. Applicants reserve the right to address any arguments presented by the Examiner in response to this point of appeal, but as the Examiner has failed to even address the means plus function elements in the final rejection, the Applicants believe that it would be improper for the Examiner to raise such new grounds of rejection for the first time on appeal.

The Examiner fails to identify any structure in the specification at paragraph 11 of the Office action mailed March 2, 2006 corresponding to the claimed protocol translator means or the encryption means. Although the Examiner does address at Page 18 the arguments regarding the Examiner's failure to identify the corresponding structure that were set out in detail in the Response mailed August 5, 2005, in what the Examiner has chosen to characterize as “Issue no. 6,” the Examiner has steadfastly refused to address the issues that were actually raised in that response, and merely states that “Rogge does teach a multi-terminal POS system design which is interpreted to receive credit transaction data from two or more point of sale systems which can use different transmission protocols associated with a different credit authorization

system and receiving responses to the credit transactions in col. 3, line 51-col. 4, line 36 and col. 5, line 28-col. 6, line 55.” As such, the Examiner’s response is defective at least for the reason that there has been no identification of the corresponding structure in the specification or discussion of where Rogge discloses that structure or an equivalent, as required under M.P.E.P. 2182. For example, corresponding structure in the specification includes method step 702 as performed by remote hub system 102 in Figure 3, which allows credit transaction data to be received from two or more point of sale systems in one of two or more transmission protocols, each transmission protocol associated with a different credit authorization system, and forming a single credit transaction data message – as such, any given request can be in one of two or more different transmission protocols, and requests in two different protocols can be formed into a single message. The discussion in the Response mailed August 5, 2005 is repeated here, explaining why the sections of Rogge relied on by the Examiner fail to disclose this structure:

1. Col. 3, line 51 through col. 4, line 36: This section does not disclose receiving the credit transaction data from two or more point of sale systems according to two or more different transmission protocols, each transmission protocol associated with a different credit authorization system, and forming a credit transaction data message. Instead, it discloses individually threaded messages:

In such a system designed according to the invention, an individual authorization request from one terminal connected to the store controller can be initiated before a response is received on an authorization request initiated from another of the terminals connected to the store controller. That is, each individual transaction need not queue up and wait for responses to previous transactions before that individual transaction is sent to the FEP. This is a multi-threaded protocol which significantly reduces transaction queuing and greatly speeds POS transactions.

(Rogge, col. 4, lines 7-16). How could two or more authorization requests be used to form a single credit transaction data message when “an individual authorization request from one terminal connected to the store controller can be initiated before a response is received on an authorization request initiated from another of the terminals connected to the store controller?” Clearly, it cannot. Furthermore, nothing in this section refers to receiving the credit transaction data from two or more point of sale systems according to two or more different transmission protocols, each transmission protocol associated with a different credit authorization system.

2. Col. 5, lines 28 through 50: This section only discusses the architecture of multiple POS terminals connected to a central store controller. No discussion about the messaging protocols between the POS terminals and the central store controller is provided.

3. Col. 5 line 59 through col. 6, line 55: This section discusses connections between the controller and a front-end processor, and teaches away from two or more different transmission protocols, each transmission protocol associated with a different credit authorization system: “if the FEP/host 29 is a system run by Exxon Corporation, then it would typically include software to provide authorization responses for transactions using an Exxon credit or Exxon debit card.” Thus, only a single type of credit authorization system is anticipated by Rogge. Furthermore, even where Rogge discloses that different credit authorization systems arguably could be used together, it makes it clear that the transactions are individually processed in response to the individual threads that were previously discussed: “For other cards, such as MasterCard, Visa, or a bank debit card, the FEP/host 29 communicates with other host systems as will be described later, sending authorization requests and receiving responses from those hosts, and then sending the responses downline to the controller 24.”.

As has been clearly explained, Rogge fails to disclose the claimed structure or any equivalent, and uses a thread architecture that requires a single thread for each authorization request. The Examiner has failed to even identify what structure he considers to be the corresponding structure, much less to explain why the structure disclosed in Rogge anticipates. It is interesting to further note that the Examiner did not change the basis for rejection even after the protocol translator means was added to the claim, further evidence that the Examiner has failed to properly base the rejection on the corresponding structure in the specification. Finally, as noted below in regards to claim 24, the Examiner admits at page 14 of the Office action mailed March 2, 2006 that Rogge fails to disclose a protocol translator receiving the credit transaction data from each of the one or more point of sale systems according to the proprietary data format associated with each point of sale system – the very structure that the Examiner claims at page 11 of that Office action is disclosed by Rogge!

In regards to the encryption means for receiving the credit transaction data message from a protocol translator and encrypting the credit transaction data message, the Examiner does admit that Rogge fails to disclose that element, but asserts that Nair discloses such at col. 5 line 60 to col. 6, line 38, again without any identification of the corresponding structure in the specification

or analysis of the structure in Nair and whether it is the same or an equivalent. The disclosure of Nair relates to reading embossed characters from a credit card and other such functionality. In contrast, the corresponding structure of the encryption means in the specification, such as that disclosed in the encryption system 502 in Fig. 5 and described at page 16, lines 11-26, or at steps 704 and 706 of Fig. 7 and described at page 22, lines 5-15, does not involve the credit card reader whatsoever. Reversal of this rejection is required.

**7. The Examiner has not identified the corresponding structure of the means plus function elements in claim 10, and there is no such structure or an equivalent in any of the cited art.**

As to claim 10, the Examiner again failed to identify the corresponding structure for the device router means. The device router means includes at least device router 508 of remote hub system 102, whereas the cited section of Rogge discusses Fig. 2 of Rogge, which discloses that “FEP/host 29 handles the routing of the authorization request” – i.e., to the authorization system or to the controller 24, not to the individual point of sale terminals. As device router 508 of remote hub system 102 is coupled through remote hub system 102 directly to the point of sale systems 104a through 104c of Figure 3, it is clear that the FEP/host 29 of Rogge is incapable of being the claimed device router means, which transmits “authorization data received in response to the credit transaction data message to the one or more point of sale systems.” In fact, as Rogge uses individual threads for the authorization data, routing of the authorization data to an individual point of sale system is not required. Furthermore, as the claimed structure of the device router means allows multiple authorization responses to be transmitted from gateway system 106 to remote hub 102 in a single authorization response and for the device router means to route the separate authorization responses to each corresponding point of sale terminal, the individual threading of Rogge would prohibit Rogge from being used as the claimed device router means. Reversal of this rejection by the Board is required.

**8. The Examiner has not identified the corresponding structure of the means plus function elements in claim 11, and there is no such structure or an equivalent in any of the cited art.**

In regards to claim 11, the Examiner again declined to identify the corresponding structure of the claimed management system interface means for storing a protocol module to the protocol

translator, merely citing to col. 11, line 55 to col. 12, line 51, col. 14, line 42-58, col. 15 line 64 to col. 16, line 25 and col. 17, lines 21-65 – a massive amount of text for disclosing a single claim element! Looking at each section in detail, it can be seen that col. 11, line 55 to col. 12, line 51 discusses a POS system using multi-threaded transactions; that col. 14, line 42-58 discusses step 536 of Figure 5, which deals with terminal control software; that col. 15 line 64 to col. 16, line 25 further deals with the terminal software; and that col. 17, lines 21-65 deals with the network control software. None of the cited section deals with a management system interface means for storing a protocol module to the protocol translator, which translates between data transmission protocols used by the point of sale systems to a data transmission format used to communicate between a remote hub system and a gateway. Nothing discussed in the voluminous sections cited by the Examiner remotely relates to that function. Reversal of this rejection by the Board is also required.

**9. The Examiner has not identified the corresponding structure of the means plus function elements in claims 12, 25 and 26, and there is no such structure or an equivalent in any of the cited art.**

In regards to claim 12, the Examiner again declined to identify the corresponding structure of the claimed management system interface means for storing an encryption module to an encryption system. The Examiner does admit that neither Rogge or Nair disclose the claimed management system interface means for storing an encryption module to an encryption system, but asserts that Weber discloses that element at col. 3, lines 10-67, and also that it would have been obvious to combine Rogge, Nair and Weber. However, looking at the cited section of Weber, that reference only discusses various proprietary encryption protocols that are largely incompatible, and entirely fails to discuss management system interface means for storing an encryption module to an encryption system, much less how that would be combined with the other claim elements or any motivation for doing so. As noted by Weber at col. 3, lines 42-45, one “of ordinary skill in the art readily comprehends that any of the general-purpose secure communication protocols can be substituted for the SSL transmission protocol without undue experimentation.” The SSL transmission protocol and other general-purpose secure communication protocols must remain compatible with older versions, and updates for such software are not required. As such, Weber teaches away from any combination with other art to



provide for management system interface means for storing an encryption module to an encryption system, such as that structure disclosed at Figure 8, steps 812 through 814, where it is determined whether an encryption update is being transmitted in a remote management message and is stored if it is.

In regards to claim 25, Weber is also relied on as disclosing update means for receiving an encryption update and installing the encryption update on the remote hub system at col. 65, line 16 to col. 66, line 20. The section cited by the Examiner relates to customization of the point of sale terminal, not the remote hub. Furthermore, as previously discussed, Weber teaches away from updating encryption, as all of the systems disclosed by Weber are in widespread use and would not function if updates were implemented.

In regards to claim 26, Weber is again relied on as disclosing update means for receiving an encryption update and installing the encryption update on one or more of the point-of-sale systems at col. 21, line 20 to col. 22, line 23. The cited section of Weber relates to payment capture request processing and has nothing whatsoever to do with installing encryption updates on point of sale systems. As previously discussed, the section cited by the Examiner in regards to claim 25 is actually more pertinent to point of sale system updates, but even that section fails to disclose anything related to update means for receiving an encryption update and installing the encryption update on one or more of the point-of-sale systems. Reversal of these rejections by the Board is required.

**10. The Examiner has not made a prima facie showing of obviousness in rejecting claims 9-11 and 17 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,500,890 to Rogge et al. (hereinafter “Rogge”) in view of U.S. Patent No. 5,448,047 to Nair et al. (hereinafter “Nair”).**

The failure of Rogge to disclose the corresponding structure of the protocol translator means of claims 9-11 has already been discussed. In regards to claim 17, the Examiner misstated the rejection of that claim over Rogge in view of Nair. In fact, that claim was rejected over Rogge in view of Nair and further in view of Weber. Reversal of these rejections by the Board is required.

**11. The Examiner has not made a prima facie showing of obviousness in rejecting claims 12-28 under 35 U.S.C. § 103(a) as being unpatentable over *Rogge* and *Nair* in view of U.S. Patent No. 6,178,409 to Weber et al. (hereinafter “*Weber*”).**

The failure of the Examiner to make a prima facie showing of obviousness as to the rejection of claims 12, 25 and 26 has already been discussed.

In regards to claim 13, neither *Rogge*, *Nair* or *Weber* disclose receiving credit transaction data from two or more point of sale devices, each reading credit card data from a magnetic stripe of a credit card and determining a point-of-sale device data transmission protocol to use to assemble the credit transaction data into an authorization request. As discussed, *Rogge* uses individual threaded messages for each point of sale terminal and does not determine a point-of-sale device data transmission protocol to use to assemble the credit transaction data from two or more point of sale terminals into a single authorization request. Furthermore, none of the cited art allows the authorization request, which includes credit transaction data from two or more point of sale devices, to be transmitted to the appropriate authorization system. *Rogge*’s use of single threaded messages for each point of sale terminal precludes that function from occurring. Reversal of this rejection by the Board is required.

In regards to claim 15, the Examiner asserts that *Weber* discloses encrypting the credit transaction data using an encryption module received from a hub manager at col. 13, lines 29-56 and col. 14, lines 37-67. The cited sections of *Weber* only relate to an exchange of a certificate for authentication of identity and negotiation of encryption between a customer and a merchant. Claim 13 has nothing to do with communications between customers and merchants. A point of sale device would be commonly understood to be a device used by a merchant, not a customer, and no contrary construction is used in the specification. Furthermore, the term “encryption module” is defined in the specification as something that updates the encryption procedure used to encrypt the credit transaction data. Exchange of encryption keys or negotiation of one of a different pre-existing encryption schemes is not an update of an encryption procedure.

In regards to claim 17, the Examiner admits that *Rogge* fails to teach transmitting one or more control messages to a remote hub, each control message adapted for one of two or more different point of sale devices, but asserts that 1) *Nair* discloses transmitting one or more control messages to a remote hub at col. 4 lines 20-44 and lines 54-60, and that 2) *Weber* discloses each control message adapted for one of two or more different point of sale devices “process the

control message at the remote hub” at col. 42, lines 41-50. Thus, even though Nair fails to disclose that each of the control messages transmitted to a remote hub can be adapted for one of two or more different point of sale devices, and even though Weber fails to disclose that the control messages adapted for one of two or more different point of sale devices are transmitted to a remote hub, the Examiner asserts that it is obvious to combine them with Rogge to provide the claimed invention.

Looking in detail at the cited sections proves otherwise. Nair, at the cited sections, only discloses a multiple reader terminal that reads embossed characters and magnetic stripes from a single card. There is simply no remote hub disclosed. Any reasonable interpretation of the claims must recognize that the remote hub and the two or more *different* point of sale devices are not the same single point of sale device. Likewise, Weber, at the cited section, only discloses a typical message flow between the consumer, merchant, vPOS terminal and the gateway – there is simply no control message adapted for one of two or more different point of sale devices, because Weber only discloses a single type of virtual POS terminal. Again, the Examiner has failed to meet the burden of a prima facie basis for rejection under 35 U.S.C. 103, because the prior art does not disclose all of the claimed elements.

Likewise, the Examiner’s construction of processing the control message at the remote hub; and performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device is also flawed because Weber is drawn to virtual point of sale terminals, not point of sale devices that read credit card data from a magnetic stripe of a credit card. In fact, the systems of Rogge, Weber and Nair are almost totally incompatible – Rogge is drawn to a multiple POS system, Nair is drawn to a combined magnetic stripe and embossed card reader (not two separate POS terminals), and Weber is drawn to a virtual POS system that does not even use card readers.

In regards to claim 20, the Examiner acknowledges that Rogge fails to disclose the method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises updating the remote hub with a protocol module to accommodate a new point of sale device, but asserts that Nair discloses such at col. 11, line 48 to col. 12, line 6. In fact, all that is disclosed by Nair is that a multi-reader terminal of Nair can forward messages

to other devices. Updating the remote hub with a protocol module to accommodate a new point of sale device is simply not disclosed.

In regards to claim 22, the Examiner acknowledges that Rogge fails to disclose a remote hub system coupled to a communications medium, the remote hub system receiving the credit transaction data from one or more of the point of sale systems, translating the credit transaction data from the proprietary data format to a predetermined data format, encrypting the translated credit transaction data, and transmitting the translated encrypted credit transaction data over the communications medium, but asserts that Weber discloses such at col. 24, lines 7-56. Weber, as discussed, relates to a virtual POS system that does not require interface to point of sale systems using proprietary data formats. All of the POS terminals of Weber use a predetermined data format that is compatible with Weber. Because Weber does not relate in any way to physical point of sale systems, which cannot be readily re-programmed, and only virtual point of sale systems, which can be easily reprogrammed as they only come into existence when they are instantiated by an operator at the start of a session, one of ordinary skill would see no motivation to combine the teachings of Weber with Rogge. The motivation cannot be provided by the teachings of the claimed invention, or using the claimed invention as a blueprint – one would need to be motivated to combine the POS system of Rogge, which uses hardware devices, with the virtual POS system of Weber, which does not use any hardware devices. Weber, which is a voluminous 172 pages with 66 Figures, merely has this to say about conventional POS systems at col. 4, lines 10-12 “Internet-based payment solutions require additional security measures that are not found in conventional POS terminals.” There is no motivation to combine Weber with Rogge absent the teachings of the present invention, which is drawn to providing the additional security measures for Internet-based payment solutions to allow data from conventional POS terminals to be transmitted over the Internet. Reversal of the rejection of claim 22 is required.

In regards to claim 24, the Examiner admits at page 14 of the Office action mailed March 2, 2006 that Rogge fails to disclose a protocol translator receiving the credit transaction data from each of the one or more point of sale systems according to the proprietary data format associated with each point of sale system. How on earth is Rogge then capable of disclosing the claimed protocol translator means, which corresponds to the structure disclosed in the specification, so as to provide the basis for the rejection of Claim 9 under 35 U.S.C. 103? At a minimum, the Examiner's admission necessitates reversal of the rejection of claim 9.

Furthermore, as discussed, there is simply no motivation to combine Rogge with Weber, and even if they are combined, neither Rogge, Nair or Weber disclose POS terminals, virtual or otherwise, using different proprietary data formats. This rejection must also be reversed by the Board.

In regards to claim 27, the Examiner asserts that Rogge discloses one or more pre-existing point of sale systems that are configured to communicate using a public switched telephone network telephone line. Where, then, is the motivation to combine Rogge and Weber? As stated in Weber, "Internet-based payment solutions require additional security measures that are not found in conventional POS terminals." As Rogge discloses point of sale systems that are configured to communicate using a public switched telephone network telephone line or other secure communications media, where does the motivation come from to combine Weber and Rogge? Nowhere except from the teachings of the present invention. Reversal of this rejection is required.

In regards to claim 28, the Examiner asserts that Rogge discloses at col. 12, lines 54-64 a telephone backup system coupled to one or more of the point of sale systems and the hub, wherein the hub uses the telephone backup system when the communications medium is unavailable. No such back-up system is disclosed. The cited section of Rogge merely notes that various secure communications media can be used, not that the hub uses the telephone backup system when the communications medium is unavailable. In order for the hub to use telephone backup system when the communications medium is unavailable, it would need to be able to detect such unavailability as well as to reconfigure itself. Rogge fails to disclose any such functionality. Reversal of this rejection is required.

**VIII APPENDIX OF CLAIMS (37 C.F.R. 41.37(c)(8))**

The text of the claims involved in the appeal are:

Claims 1-8 (cancelled).

9. An apparatus for transmitting credit transaction data over a communications medium comprising:

protocol translator means for receiving the credit transaction data from two or more point of sale systems according to two or more different transmission protocols, each transmission protocol associated with a different credit authorization system, and forming a credit transaction data message; and

encryption means for receiving the credit transaction data message from a protocol translator and encrypting the credit transaction data message.

10. The apparatus of claim 9 further comprising device router means for transmitting authorization data received in response to the credit transaction data message to the one or more point of sale systems.

11. The apparatus of claim 9 further comprising management system interface means for storing a protocol module to the protocol translator.

12. The apparatus of claim 9 further comprising management system interface means for storing an encryption module to an encryption system.

13. A method for transmitting credit transaction data over a communications medium comprising:

receiving credit transaction data from two or more point of sale devices, each reading credit card data from a magnetic stripe of a credit card;

determining a point-of-sale device data transmission protocol to use to assemble the credit transaction data into an authorization request;

encrypting the authorization request;

transmitting the encrypted authorization request over the communications medium;

decrypting the encrypted authorization request;

determining which of two or more authorization systems is the appropriate authorization system to provide the authorization request to; and  
transmitting the authorization request to the appropriate authorization system.

14. The method of claim 13 wherein receiving the credit transaction data from the point of sale device comprises receiving the credit transaction data in accordance with one or more of an ISO 8583 protocol or a Visa-K protocol.

15. The method of claim 13 wherein encrypting the authorization request comprises encrypting the credit transaction data using an encryption module received from a hub manager.

16. The method of claim 13 wherein transmitting the encrypted authorization request over the communications medium comprises transmitting the encrypted data in an HTTP format.

17. A method for controlling the transmission of credit transaction data comprising:  
transmitting one or more control messages to a remote hub, each control message adapted for one of two or more different point of sale devices;  
processing the control message at the remote hub; and  
performing a control function on one of two or more point of sale devices that read credit card data from a magnetic stripe of a credit card at the remote hub in response to the control message if the control message is adapted for the point of sale device.

18. The method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises transmitting status data for the remote hub.

19. The method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises transmitting status data for one or more point of sale devices connected to the remote hub.

20. The method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises updating the remote hub with a protocol module to accommodate a new point of sale device.

21. The method of claim 17 wherein performing the control function at the remote hub in response to the control message comprises updating the remote hub with an encryption module.

22. A system for transmitting credit transaction data comprising:

two or more point-of-sale systems, each point-of-sale system using a proprietary data format to read credit card data from a magnetic stripe of a credit card and generate credit transaction data;

a remote hub system coupled to a communications medium, the remote hub system receiving the credit transaction data from one or more of the point of sale systems, translating the credit transaction data from the proprietary data format to a predetermined data format, encrypting the translated credit transaction data, and transmitting the translated encrypted credit transaction data over the communications medium; and

a gateway system coupled to the communications medium, the gateway system receiving the encrypted translated credit transaction data, decrypting the encrypted translated credit transaction data, and transmitting the translated credit transaction data to an authorization system.

23. The system of claim 22 further comprising:

a first authorization system coupled to the gateway system;

a second authorization system coupled to the gateway system; and

wherein the gateway system transmits the credit transaction data to the first or second authorization system based upon the translated credit transaction data.

24. The system of claim 22 wherein the remote hub system further comprises a protocol translator receiving the credit transaction data from each of the one or more point of sale systems according to the proprietary data format associated with each point of sale system.

25. The system of claim 22 wherein the remote hub system further comprises update means for receiving an encryption update and installing the encryption update on the remote hub system.



26. The system of claim 22 wherein the remote hub system further comprises update means for receiving an encryption update and installing the encryption update on one or more of the point-of-sale systems.

27. The system of claim 22 wherein the point-of-sale systems include one or more pre-existing point of sale systems that are configured to communicate using a public switched telephone network telephone line.

28. The system of claim 27 further comprising a telephone backup system coupled to one or more of the point of sale systems and the hub, wherein the hub uses the telephone backup system when the communications medium is unavailable.

**IX EVIDENCE APPENDIX (37 C.F.R. 41.37(c)(9))**

This page intentionally left blank

**X RELATED PROCEEDINGS APPENDIX (37 C.F.R. 41.37(c)(10))**

This page intentionally left blank.

Dated: September 11, 2006

Respectfully submitted,

JACKSON WALKER L.L.P.

By: 

Christopher J. Rourke  
Reg. No. 39,348

901 Main Street, Suite 6000  
Dallas, TX 75202  
Telephone: (214) 953-5990  
Facsimile: (214) 953-5822